AFFIDAVIT OF VANESSA IP

State of New York)
) ss.:
County of New York)

I, Vanessa Ip, hereby declare as follows:

1. I am an Investigator with the Internet Bureau of the New York State Attorney General's Office. My work address is 120 Broadway, Third Floor, New York, New York 10271. I make this declaration based upon my personal knowledge of the facts set forth herein.

2. Between November 2004 and September 2005, I conducted a number of investigative tests, through Attorney General office undercover computers, to record "spyware" or "adware" from DirectRevenue, LLC. ("Direct Revenue") being uploaded and installed onto computers without notice or consent. I have set forth the results of those tests herein, including the websites from which the downloads occurred, and the disclosures – or lack thereof – presented to users. I have attached as exhibits hereto all relevant screen shots of these tests.

Faster XP download

3. On May 11, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive, using the programs Ad-Aware SE Personal Edition[1] ("Ad-Aware) and Spybot Search &

[1] Ad-Aware is an anti-spyware program distributed by Lavasoft. According to the company's website (www.lavasoftusa.com), "Ad-Aware is designed to provide advanced protection from known Data-mining, aggressive advertising, Parasites, Scumware, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components." Ad-Aware has been awarded PC Magazine Editors' Choice Award by a panel of PC Magazine editors and leading industry experts.

Destroy[2] ("Spybot"). At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit A-1, which are true and correct images of the result screens.*)

4. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit A-2, which is a true and correct image of the window.*)

5. I next opened the C:\WINDOWS folder to view a listing of the files located within that folder. (*See Exhibit A-3, which are true and correct images of the windows.)*

6. I next opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit A-4, which is a true and correct image of the browser window.*)

7. In the address bar, I typed the website address <www.fasterxp.com> and was directed to the FasterXP homepage. The page described FasterXP's software and contained a large button marked "Free Download." The page further promised that the software was "100% Spyware free." There was also a fineprint statement that "By clicking the "Free download" button above and downloading FasterXP, I accept and agree to abide by the End User License Agreement." Neither this page – nor any other leading up to the download and installation of the FasterXP software – made any mention of bundled spyware programs. (*See Exhibit A-5, which is a true and correct image of the browser window.*)

8. I clicked on the link to the "End User License Agreement" and a new browser window launched (http://198.87.3.82/fasterxp/eula.html) which contained the FasterXP End User License Agreement, viewable over 12 screens. On the fourth page of this agreement, a

---

[2] Spybot Search & Destroy is a program designed to "detect and remove spyware of different kinds from your computer," according to its website (www.spybot.info). The software was named the best "Anti-Spyware Scanner" of 2004 by PCWorld.com. In early tests, the Spybot scans invariably generated five entries for "DSO Exploit" which was not indicative of any resident spyware programs.

small statement read, “Please read and understand the ABetterInternet End user license agreement before installing FasterXP, by clicking the following link : http://www.abetterinternet.com/policies.htm.” *(See Exhibit A-6, which are true and correct images of the browser window.*)

9. I closed the End User License Agreement window and on the FasterXP homepage, clicked on the “Free Download” button. Two File Download windows popped up, indicated that I would be downloading the application “fasterxp.exe” from 187.87.3.82. (*See Exhibit A-7, which is a true and correct image of the windows.*)

10. I continued through the process of saving the “fasterxp.exe” application by clicking on the “Save” button and indicating a location for the download. A window popped up to indicate that the download was complete. (*See Exhibit A-8, which are true and correct images of the windows.*)

11. I clicked on the “Open” button to launch the FasterXP installation and a “FasterXP Free: Downloading” window popped up, indicating the deletion of temporary file “WebRebates.xxx”. (*See Exhibit A-9, which is a true and correct image of the windows.*)

12. A new window opened offering a free evaluation of “Optisoft Internet Project, S.L. FasterXP” software. (*See Exhibit A-10, which is a true and correct image of the windows.*)

13. Although it was not required to view the “End-User Terms and Conditions on the Softwrap web site” to advance, I clicked on the link to the terms and was directed to the webpage containing the “Softwrap End-User Licence [*sic*] Agreement,” (www.softwrap.com/tc2.asp), viewable over six screens. None of the screens contained any mention of or reference to Direct Revenue’s spyware. (*See Exhibit A-11, which are true and correct images of the browser*

window.)

14. I returned to the FasterXP installation window and advanced by clicking the "Next" button. I was offered the option to "Try Now" or "Buy Now" the "Optisoft Internet Project, S.L. FasterXP" software. (*See Exhibit A-12, which is a true and correct image of the window.*)

15. I opted to "Try "Optisoft Internet Project, S.L. FasterXP" free of charge." The program checked the Windows Version, and I continued to advance through the installation by clicking "Next" through the next six screens (Internet Connection, "Last Access" Attribute, Old 8.3 File Names, Contiguous File Allocation Size, I/O Page Limit and Menu Reaction Speed), leaving all the settings at the defaulted "Optimize" setting. (*See Exhibit A-13, which are true and correct images of the windows.)*

16. I received a pop-up indicating that the FasterXP "Optimization [was] successful." I clicked "Cancel" to close FasterXP. (*See Exhibit A-14, which is a true and correct image of the pop-up window.)*

17. After closing all browser windows, I opened the C:\Program Files\ folder, which indicated that three new files had been added after the FasterXP installation: FasterXP, MySearch and Web_Rebates. Direct Revenue's Aurora program was not listed. *(See Exhibit A-15, which are true and correct images of the windows.*)

18. I proceeded to the C:\WINDOWS folder, which indicated that several files had been added to that directory since the FasterXP installation, including the Direct Revenue files "svcproc" and "Nail." The "Date Modified" listed for these files was August 13, 2003 and March 29, 2005, respectively. *(See Exhibit A-16, which are true and correct images of the*

windows.)

19. I opened a new browser window through Internet Explorer and found the start page changed to <www.fasterhomepage.com>. A pop-up window titled "Aurora" displayed an advertisement for "free Registry Cleaner software" from SysTweak.com. (*See Exhibit A-17, which is a true and correct image of the browser and pop-up window.*)

20. Upon visiting other websites such as <www.msnbc.com>, <www.nypost.com>, <www.hotels.com> and <www.yahoo.com>, additional "Aurora" pop-up windows appeared. The pop-ups displayed advertisements for companies such as Orbitz, Expedia, CarsDirect and online casino and poker site <www.888.com>. For the ten websites I visited, ten Aurora pop-up advertisements loaded over fourteen minutes. (*See Exhibit A-18, which are true and correct images of the browser and pop-up windows.*)

21. I entered the Windows "Add or Remove Programs" utility to view the list of currently installed programs. The listing included "FasterXP" and additionally, "My Search Bar," "Search Assistant - My Search" and "Web Rebates (by TopRebates.com)." Direct Revenue's Aurora program was not listed. (*See Exhibit A-19, which is a true and correct image of the window.*)

22. I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 69 objects, 39 attributable to VX2[3], including registry keys and values, files, a running process and a folder. (*See Exhibit A-20, which are true and correct images of the relevant scan results.*)

---

[3] "VX2" is the name of an early variant of Direct Revenue's software. Ad-Aware usually identifies all Direct Revenue spyware files and objects as "VX2."

23. I then ran a scan for existing spyware on the unit's hard drive using Spybot. That scan identified 13 problems, including one entry identifying "AbetterInternet."[4] (*See Exhibit A-21, which is a true and correct image of the relevant scan results.*)

24. Taking no further action, I re-ran the scans for spyware the following day. This time, the Ad-Aware scan identified 88 objects, 41 attributable to VX2, including registry keys and values, files, a running process and a folder. The Spybot scan identified 8 new problems: 21 in total, including the previous entry identifying "AbetterInternet." (*See Exhibit A-22, which are true and correct images of the scan results.*)

25. Through the Windows "Add or Remove Programs" utility , I selected the "Change/Remove" option to remove the FasterXP program. A confirmation window appeared, and I clicked the "Uninstall" button to proceed with the uninstall. The window indicated when the process was complete. (*See Exhibit A-23, which are true and correct images of the uninstall process.*)

26. I continued using the Windows "Add or Remove Programs" utility to remove the three other programs added after the FasterXP download: "My Search Bar," "Search Assistant - My Search" and "Web Rebates (by TopRebates.com)." Each time, I received confirmation that the uninstall had been completed successfully, or that the program would be completely uninstalled after the next reboot. (*See Exhibit A-24, which are true and correct images of the uninstall processes.*)

27. I then re-ran scans for existing spyware. The Ad-Aware scan identified 70

---

[4] A Better Internet (BetterInternet, LLC) is a division of Direct Revenue. Spybot Search & Destroy often identifies Direct Revenue spyware files and folders as "AbetterInternet."

objects, 41 still attributable to VX2. The Spybot scan identified 15 problems, including "AbetterInternet." (*See Exhibit A-25, which are true and correct images of the relevant scan results.*)

28. After instructing Ad-Aware and Spybot to remove all Direct Revenue spyware, I rebooted the computer and re-ran the scan. Ad-Aware identified 29 critical objects, *all* of which were attributable to VX2. " (*See Exhibit A-26, which are true and correct images of the scan results.*)

29. I again instructed Ad-Aware to remove all VX2 objects and files. I then opened an Internet Explorer browser window to find the start page still set to <www.fasterhomepage.com>. By visiting websites such as <www.nytimes.com>, <www.priceline.com>, <www.sony.com> and <www.dell.com>, I received "Aurora"-branded pop-up advertisements for companies such as Hotwire, United Airlines, Rewards Venue and two separate anti-virus/anti-spyware companies. I also received two separate ads for Priceline.com. In fact, I was served with an Aurora pop-up advertisement for every one of the ten URLs I visited. (*See Exhibit A-27, which are true and correct images of the browser and pop-up windows.*)

30. I re-ran scans for existing spyware. Despite having removed the critical objects twice previously, the Ad-Aware scan identified 50 new critical objects, 32 attributable to VX2 and 1 identifying a Windows Vulnerability. (*See Exhibit A-28, which are true and correct images of the scan results.*)

31. I attempted to remove the identified objects through Ad-Aware, but the program indicated that two items could not be removed. (*See Exhibit A-29, which are true and correct*

images of the windows.)

32. I closed Ad-Aware, and on the Windows Desktop, received a File Download window for "Nail.exe" from C:\WINDOWS. (*See Exhibit A-30, which is true and correct image of the Desktop.*)

33. I clicked "Cancel" to reject the "Nail.exe" download, rebooted the computer and re-ran the scan for spyware. On this fourth attempt, Ad-Aware identified 31 new critical objects, 30 attributable to VX2. (*See Exhibit A-31, which are true and correct images of the scan results.*)

34. After removing the identified objects through Ad-Aware, I ran the Spybot scan for existing spyware. The scan identified 4 problems, which I also removed. (*See Exhibit A-32, which is a true and correct image of the scan results.*)

35. I closed all open windows and without taking further action, I returned to the computer six days later, on May 18, 2005. Upon opening the Internet Explorer browser window, I found the start page still set to <www.fasterhomepage.com>, and was promptly served with an Aurora-branded pop-up advertisement for SysTweak.com's Registry Cleaner. I proceeded to visit websites for Expedia, BMW and Dell, and each time was served with an Aurora pop-up. (*See Exhibit A-33, which are true and correct images of the browser and pop-up windows.*)

36. I re-ran scans for existing spyware for the fifth time in one week. On this scan, Ad-Aware identified 124 new critical objects, 41 attributable to VX2. Spybot identified 36 problems, including AbetterInternet. (*See Exhibit A-34, which are true and correct images of the relevant scan results.*)

A Better Internet "Atomic Clock" download

37. On January 13, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware. At that time, the program indicated the hard drive to be free of spyware. (*See Exhibit B-1, which are true and correct images of the result screens.)*

38. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit B-2, which is a true and correct image of the window.)*

39. I next opened Internet Explorer and directed the browser to <www.abetterinternet.com>. Neither this page – nor any other leading up to the download and installation of the Atomic Clock software – made any mention of bundled spyware programs. (*See Exhibit B-3, which are true and correct images of the browser window.*)

40. Although not required to proceed with the downloads, I scrolled to the lower left-most corner of the homepage to click on the "EULA" link. I was directed to <www.abetterinternet.com/policies.htm> and received an error message that "The page cannot be displayed." (*See Exhibit B-4, which is a true and correct image of the browser window*.)

41. I hit "Back" on the browser window to return to the ABetterInternet homepage, and clicked on the "download now!" link under the "Atomic Clock" option. An ActiveX dialog offering the installation of "Atomic Clock" distributed by "BetterInternet" appeared on the screen over a newly launched browser window. The dialog indicated that clicking "Yes" would acknowledge acceptance of BetterInternet's Consumer Policy Agreement. (*See Exhibit B-5, which is a true and correct image of the browser and ActiveX dialog windows.*)

42. Although viewing the Consumer Policy Agreement was not required to proceed with the installation, I clicked on the link to the agreement and a new browser window launched,

again directing me to the error page for <www.abetterinternet.com/policies.htm>, where no agreement was viewable.

43. I closed the error window and clicked "Yes" in the ActiveX dialog to proceed with the Atomic Clock installation. The dialog closed and the browser window beneath indicated that the install was in progress. (*See Exhibit B-6, which is a true and correct image of the browser window.*)

44. The Atomic Clock Sync Installation Wizard launched and I proceeded with the setup by clicking "Next" through three windows: "Welcome," "Choose Destination Location" and "Start Installation." (*See Exhibit B-7, which are true and correct images of the windows.*)

45. The final window indicated that the installation was complete. I clicked "Finish" to exit the installation. (*See Exhibit B-8, which is a true and correct image of the window.*)

46. I closed all open browser windows, revealing the Windows Desktop to which the Atomic Clock Sync icon was newly added. (*See Exhibit B-9, which is a true and correct image of the Desktop.*)

47. I proceeded to the C:\Program Files directory to view a listing of the files located within that folder, and found that the "Atomic Clock Sync" folder had been added. Direct Revenue's Ceres program was not listed. (*See Exhibit B-10, which is a true and correct image of the window.*)

48. I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 21 objects, almost all attributed to VX2. (*See Exhibit B-11, which are true and correct images of the scan results.*)

49. I removed all items identified by Ad-Aware and without further action, returned to

the computer the following day to repeat the scans for spyware. Despite having previously removed all spyware the day before, Ad-Aware identified 3 new critical objects, attributed to VX2. (*See Exhibit B-12, which are true and correct images of the scan results.*)

50. I entered the Windows "Add or Remove Programs" utility for a listing of the programs installed on the hard drive. In addition to the Atomic Clock Sync, there was an entry for "CERES." (*See Exhibit B-13, which is a true and correct image of the window.*)

51. I removed the Atomic Clock Sync program by launching the Uninstall Wizard through the Windows "Add or Remove Programs" utility . (*See Exhibit B-14, which are true and correct images of the windows.*)

52. After removing the Atomic Clock Sync program, the CERES program remained listed among the installed programs. (*See Exhibit B-15, which is a true and correct image of the window.*)

53. I returned to the C:\Program Files directory to view a listing of the files located within that folder, and found that the "Atomic Clock Sync" folder had not been deleted, despite my having removed the program through the Windows "Add or Remove Programs" utility . (*See Exhibit B-16, which is a true and correct image of the window.*)

54. I opened the C:\Program Files\Atomic Clock Sync folder to view its contents and was able to locate and launch the Atomic Clock Sync program. (*See Exhibit B-17, which are true and correct images of the windows.*)

My Panic Button download

55. On May 5, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard

drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit C-1, which are true and correct images of the result screens.)*

56. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit C-2, which is a true and correct image of the window.)*

57. Within the C:\Program Files folder, I opened the Common Files folder to view a listing of the six files it contained. *(See Exhibit C-3, which is a true and correct image of the window.)*

58. Next, I opened the C:\WINDOWS folder to view a listing of the files located within that folder. *(See Exhibit C-4, which are true and correct images of the windows.)*

59. I opened Internet Explorer and directed the browser to <www.mypanicbutton.com>. Neither this page – nor any other leading up to the download and installation of the Atomic Clock software – made any mention of bundled spyware programs. *(See Exhibit C-5, which is a true and correct image of the browser window.)*

60. At the top of the MyPanicButton.com homepage, I clicked on the link to "Free Trial." An ActiveX dialog offering the installation of "My Panic Button" distributed by "BetterInternet" appeared on the screen over a newly launched browser window. The dialog indicated that clicking "Yes" would acknowledge acceptance of BetterInternet's Consumer Policy Agreement. (*See Exhibit C-6, which is a true and correct image of the browser and ActiveX dialog windows.*)

61. Although viewing the Consumer Policy Agreement was not required to proceed with the installation, I clicked on the link to the agreement. A new browser window launched, <www.abetterinternet.com/policies.html>, which contained the BetterInternet End User License

Agreement," viewable over seven screens. (*See Exhibit C-7, which are true and correct images of the window.*)

62. I closed the window and clicked "Yes" in the ActiveX dialog to proceed with the My Panic Button installation. The dialog closed and the browser window beneath indicated that the download was in progress. In addition, a new window launched, directing me to click "Yes" if prompted with a security box to complete the My Panic Button download. (*See Exhibit C-8, which are true and correct images of the browser windows.*)

63. A new ActiveX dialog offering the installation of "My Panic Button" distributed by "BetterInternet" appeared on the screen. This dialog box did not reference BetterInternet's Consumer Policy Agreement. As directed, I clicked "Yes" in the dialog to complete the download of the "My Panic Button" software. (*See Exhibit C-9, which is a true and correct image of the browser and ActiveX dialog windows.*)

64. The My Panic Button Setup Wizard launched with a "Welcome" screen and I proceeded with the setup by clicking "Next," which led to the MyPanicButton License Agreement dialog. The window could not be enlarged, but I was able to view the entire agreement by scrolling through nine screens. The agreement made no mention of or reference to bundled spyware programs. (*See Exhibit C-10, which are true and correct images of the windows.)*

65. After accepting the terms, I continued through the My Panic Button setup by clicking "Next" through the next three windows, leaving all settings at default: "Select Destination Directory," "Select Start Menu Folder" and "Select Additional Tasks." At the "Ready to Install" window, I clicked on "Install" to begin the My Panic Button installation. (*See*

Exhibit C-11, which are true and correct images of the windows.)

66. The dialog indicated the progress of the installation, and I clicked on "Finish" to exit the Setup and close the window. (*See Exhibit C-12, which are true and correct images of the windows.*)

67. A new window opened, indicating 15 days left for the Trial Evaluation of My Panic Button. I opted to "Continue Trial," launching the My Panic Button program. (*See Exhibit C-13, which are true and correct images of the windows.*)

68. I attempted to close the My Panic Button program and received a prompt asking, "Are You Sure You Want to Exit?" I clicked "OK" to confirm and closed all open browser windows. (*See Exhibit C-14, which are true and correct images of the windows.*)

69. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that one new folder had been added during the software download process: My PanicButton. Direct Revenue's VX2 program was not listed. *(See Exhibit C-15, which is a true and correct image of the window.)*

70. I next opened the C:\Program Files\Common Files folder and found that one new file had been added there as well: Better Internet, Inc. I opened the Better Internet, Inc folder to view a listing of its contents. The "Date Modified" listed for each of the files ranged from October 19, 1998 to April 27, 2003. *(See Exhibit C-16, which are true and correct images of the windows.)*

71. I proceeded to the C:\WINDOWS directory and found that several new files had been added to the directory since the installation of My Panic Button, including the Direct Revenue file "host.dll." *(See Exhibit C-17, which are true and correct images of the directory.)*

72. I exited the C:\WINDOWS directory and ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 44 objects, including many VX2 and Transponder[5] registry keys and files. Spybot identified 11 problems, including 3 entries for "VX2/?," 6 entries for "VX2/f" and 1 entry for "VX2/h.ABetterInternet." (*See Exhibit C-18, which are true and correct images of the scan results.*)

Soft Explode "Luke the Screen Washer" download

73. On May 10, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit D-1, which are true and correct images of the result screens.)*

74. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit D-2, which is a true and correct image of the window.)*

75. Next, I opened the C:\WINDOWS folder to view a listing of the files located within that folder. *(See Exhibit D-3, which are true and correct images of the windows.)*

76. Within the C:\WINDOWS folder, I opened the System32 folder to view a listing of its contents. *(See Exhibit D-4, which are true and correct excerpted images of the window.)*

77. I launched Internet Explorer and directed the browser to the Soft Explode Free Software Portal at <www.softexplode.com>. *(See Exhibit D-5, which are true and correct images of the browser window.)*

78. Under the "Desktop Enhancements" section, I clicked on the "Screensavers" link

---

[5] Direct Revenue's spyware is sometimes identified as "Transponder" by anti-spyware applications.

and was directed to the "Screensavers Downloads" at SoftExplode.com. *(See Exhibit D-6, which is a true and correct excerpted image of the browser window.)*

79. I clicked on the link for "Cartoon & Anime" link and was directed to the Cartoon & Anime Category Downloads at SoftExplode.com. *(See Exhibit D-7, which are true and correct excerpted images of the browser window.)*

80. I selected "Luke The Screen Washer Summer 1.1" and was directed to the download page for that screen saver, which identified the publisher as BetterInternet. *(See Exhibit D-8, which are true and correct images of the browser window.)*

81. I clicked on the link to "Download this Item!" and the next page indicated that the site was contacting a third party download site.. *(See Exhibit D-9, which are true and correct images of the browser window.)*

82. Within moments, the "File Download" window appeared. I clicked on the "Save" button to download the files from software-files.download.com. *(See Exhibit D-10, which is a true and correct image of the windows.)*

83. The "Save As" window appeared, and I designated a location for the "luke_summer" Compressed (zipped) Folder. *(See Exhibit D-11, which is a true and correct image of the windows.)*

84. After clicking on the "Save" button, the download process was initiated. The window indicated the progress of the download and when it was complete. *(See Exhibit D-12, which are true and correct images of the windows.)*

85. I clicked "Open" to enter the "luke_summer.zip" folder and set the task to "Extract all files." *(See Exhibit D-13, which are true and correct images of the windows.)*

86. Doing so launched the Extraction Wizard, and after clicking "Next" through the "Welcome" and "Select Destination" windows, the extraction was complete. *(See Exhibit D-14, which are true and correct images of the windows.)*

87. I clicked "Finish" to exit the Extraction Wizard and was able to view the contents of the newly extracted "luke_summer" folder. *(See Exhibit D-15, which is a true and correct image of the windows.)*

88. I launched the "luke.exe" screen saver by double-clicking on the "luke" icon. A C:\WINDOWS\System32\cmd.exe DOS prompt window popped up, followed by a "Screen Saver Installation" window. *(See Exhibit D-16, which are true and correct images of the windows.)*

89. The "Screen Saver Installation - Welcome" dialog box opened. I clicked "Install>" to proceed with the Setup program, and then "Close" to complete the installation. *(See Exhibit D-17, which are true and correct images of the windows.)*

90. The Windows Display Properties window launched, and I clicked "OK" to set the "Luke-The Screen Washer" Screen Saver. *(See Exhibit D-18, which is a true and correct image of the windows.)*

91. After closing all windows, I opened the C:\Program Files\ folder, which indicated the same seventeen files as prior to the screen saver download. Neither Luke the Screen Washer nor Direct Revenue's Offer Optimizer program was listed. *(See Exhibit D-19, which is a true and correct image of the window.*)

92. I proceeded to the C:\WINDOWS folder, which indicated that several files had been added to that directory since the screen saver download, including the Direct Revenue files

"twaintec.dll" and "preInsTT." The "Date Modified" for these files was November 12, 2004 and May 4, 2004, respectively. *(See Exhibit D-20, which are true and correct images of the windows.)*

93. I next opened the C:\WINDOWS\System32 folder, which also indicated the addition of files, including "Luke-The Screen Washer" Screen Saver, and the Direct Revenue files "webomta" and "polall1m." The "Date Modified" listed for these files was May 10, 2005 and July 27, 2004. *(See Exhibit D-21, which are true and correct excerpted images of the windows.)*

94. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 166 new critical objects, including many VX2 registry keys and values, files, a folder and two running processes. Spybot identified 44 problems, including 2 entries for "AbetterInternet," 5 entries for "Callinghome.biz" and 5 entries for "Phynix."[6] (*See Exhibit D-22, which are true and correct images of the relevant scan results.*)

95. I returned to the C:\WINDOWS\System32 folder, and found that the modified date of the previously identified "webomta" file was altered from 05/10/2005 4:05 PM to 02/19/2003 1:30AM. *(See Exhibit D-23, which is a true and correct image of the window.)*

96. I closed the C:\WINDOWS\System32 folder and launched Internet Explorer, which was set to open <www.msn.com>. Upon loading that page, a pop-up window promptly displayed an advertisement for "Registry Cleaner" by SysTweak.com. Additional surfing yielded pop-up ads for The Shield 2005/PCSecurityShield, ConsumerIncentivePromotions, SpySpotter

[6] Direct Revenue's spyware is sometimes identified as "Callinghome.biz" or "Phynix" by anti-spyware applications.

and yet another anti-spyware application. (*See Exhibit D-24, which are true and correct images of the browser and pop-up windows.*)

97. In addition, visiting <www.site59.com>, <www.onetravel.com> and <www.expedia.com>, each yielded a pop-up advertisement from offeroptimizer.com for TripReservations.com, Priceline.com and Expedia.com, respectively. (*See Exhibit D-25, which are true and correct images of the browser and pop-up windows.*)

My Tracks Eraser download

98. On July 6, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit E-1, which are true and correct images of the result screens.)*

99. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit E-2, which is a true and correct image of the window.)*

100. Next, I opened the C:\WINDOWS folder to view a listing of the files located within that folder. *(See Exhibit E-3, which are true and correct images of the windows.)*

101. I launched Internet Explorer and directed the browser to the MyTracksEraser Homepage at <www.mytrackseraser.com>. Neither this page – nor any other leading up to the download and installation of the Atomic Clock software – made any mention of bundled spyware programs. An ActiveX dialog offering an unnamed distribution by "Holistyc Limited" appeared on the screen. (*See Exhibit E-4, which is a true and correct image of the browser and ActiveX dialog windows.*)

102. Although it was not required to advance, I clicked on the link "Click Yes/Run if

you agree to the EULA" and a new window launched containing the "BETTERINTERNET END USER LICENSE AGREEMENT" at <www.dollars4traffic.com/eula.htm>. The agreement was viewable in its entirety over sixteen screens. (*See Exhibit E-5, which are true and correct images of the browser window.*)

103. I closed the BetterInternet EULA window and returned to Holistyc Limited ActiveX dialog box. I clicked "No" to reject the download and the dialog box closed. (*See Exhibit E-6, which are true and correct images of the window.*)

104. On the MyTracksEraser Homepage, I clicked on the link to "DOWNLOAD NOW 100% FREE." The File Download window appeared, indicating the download from <www.mytrackseraser.com>. (*See Exhibit E-7, which is a true and correct image of the window.*)

105. I clicked on "Save" and the "Save As" window appeared, through which I designated a location for the "setup.exe" file. *(See Exhibit E-8, which is a true and correct image of the window.)*

106. The dialog box indicated when the download was complete. *(See Exhibit E-9, which is a true and correct image of the window.)*

107. I clicked "Open" to launch MyTracksEraser and the program opened in a new window. *(See Exhibit E-10, which is a true and correct image of the window.)*

108. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 89 new critical objects, including 34 attributed to VX2 registry keys and values, files, a folder and a running process. Spybot identified 33 problems, including 2 entries for "AbetterInternet" and 1 entry for "Holistyc." (*See Exhibit E-11, which are true and correct*

images of the relevant scan results.)

109. I closed the Ad-Aware and Spybot programs and launched Internet Explorer. Over twenty minutes of surfing on sites such as <www.msn.com>, <www.ford.com> and <www.fox.com>, I received six Aurora-branded pop-up advertisements, including two for Internet security programs. (*See Exhibit E-12, which are true and correct images of the browser and pop-up windows.*)

110. After closing all windows, I opened the C:\Program Files\ folder, which indicated no additions to the seventeen previous files. Neither MyTracksEraser nor Direct Revenue's Aurora program was listed. *(See Exhibit E-13, which is a true and correct image of the window.*)

111. I proceeded to the C:\WINDOWS folder, which indicated that several files had been added to that directory since the MyTracksEraser installation, including the Direct Revenue files "svcproc," Nail," and "vsvwrizgi." Although these files had just been installed, the "Date Modified" listed for the programs was February 26, 2005, May 9, 2002 and April 17, 2002, respectively. *(See Exhibit E-14, which are true and correct images of the windows.*)

112. I closed all windows and without taking further action, returned to the same computer one week later on July 13, 2005. On the Windows Desktop, I received a File Download pop-up window for "Nail.exe" from C:\WINDOWS. (*See Exhibit E-15, which is true and correct image of the Desktop.*)

113. I clicked "Save" to download the file, and in the "Save As" window, designated a location for the "Nail" application. (*See Exhibit E-16, which is true and correct image of the window.*)

114. A dialog box indicated when the download was complete. (*See Exhibit E-17,*

which is true and correct image of the window.)

115. I clicked open to launch the application, and the dialog box closed, with no further indication of the "Nail.exe" program. (*See Exhibit E-18, which is true and correct image of the Desktop.*)

116. I opened the Windows "Add or Remove Programs" utility , which contained no listing of the "Nail.exe" program. Highlighting the "ABI Network- A Division of Direct Revenue" program, I clicked on the Change/Remove button. (*See Exhibit E-19, which is true and correct image of the window.*)

117. A new window launched from the hard drive at C:\WINDOWS\abiuninst.htm, indicating that ABI Network software could be "safely and completely removed by going to www.mypctuneup.com to get the uninstall tool." (*See Exhibit E-20, which is true and correct image of the window.*)

118. Although not necessary or required to advance, I clicked on the EULA link at the lower left corner of the window. A new Internet Explorer window launched into <www.abetterinternet.com/policies.htm>, containing the "BETTERINTERNET END USER LICENSE AGREEMENT." (*See Exhibit E-21, which are true and correct images of the window.*)

119. At the bottom of the EULA page, I clicked on the link to "Uninstall", launching a new browser window directed to <www.mypctuneup.com>. *(See Exhibit E-22, which are true and correct images of the browser window.)*

120. On the myPCtuneup homepage, I clicked on the link to "FREE uninstall program" and was directed to <www.mypctuneup.com/evaluate.php>, a web page providing the instruction

for the removal of Better Internet software. *(See Exhibit E-23, which are true and correct images of the browser window.)*

121. I clicked on the orange "DOWNLOAD" button under "STEP 1 - DOWNLOAD" and the "File Download" window appeared. *(See Exhibit E-24, which is a true and correct image of the windows.)*

122. I clicked on the "Save" button to download "uninstaller_exe.php" from <www.mypctuneup.com> and the "Save As" window appeared. I designated a location for the MyPCUninstaller application and clicked "Save" again. *(See Exhibit E-25, which are true and correct images of the windows.)*

123. The download process was initiated and within moments, the download window indicated that the download was complete. *(See Exhibit E-26, which is a true and correct image of the window.)*

124. I clicked "Open" to launch the MyPCTuneUp uninstall program. A new window opened with the "Welcome" message, indicating that the program would remove ABI Network advertising software. *(See Exhibit E-27, which is a true and correct image of the window.)*

125. I clicked "Next" to proceed with the uninstall. I was then prompted to enter the security code generated on the screen. I entered this code and clicked "Submit". *(See Exhibit E-28, which is a true and correct image of the window.)*

126. The next window indicated that the code had been verified, and that the uninstall process would continue. I clicked on the "Delete" button to proceed with the process. *(See Exhibit E-29, which is a true and correct image of the window.)*

127. A window popped up indicating that "Uninstall is running" and another when the

uninstall was completed. Upon clicking the "Finish" button, another message appeared indicating that the computer must be restarted to complete uninstallation. I clicked Yes" to restart the machine. *(See Exhibit E-30, which are true and correct images of the windows.)*

ThePaymentCentre.com "Holistyc" download

128. On June 24, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit F-1, which are true and correct images of the result screens.)*

129. I then opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit F-2, which is a true and correct image of the window.)*

130. I proceeded to open the C:\WINDOWS folder to view a listing of the files located there. *(See Exhibit F-3, which are true and correct images of the windows.)*

131. Finally, within the C:\WINDOWS folder, I opened the System32 folder to view a listing of its contents. *(See Exhibit F-4, which are true and correct excerpted images of the window.)*

132. I launched Internet Explorer and directed the browser to the Google search engine at <www.google.com>. I typed "holistyc" into the search bar and hit "Search." Among the results, the final listing on the first page was for a page titled "Downloading Holistyc", located at <www.thepaymentcentre.com/build/dl.asp?id=720&affid=>. *(See Exhibit F-5, which is a true and correct image of the search results window.)*

133. I clicked on the "Downloading Holistyc" link and was directed to a page over which an ActiveX dialog box appeared asking if I wanted to install and run

"http://www.thepaymentcentre.com/build/vciewer.cab" distributed by Holistyc Limited. *(See Exhibit F-6, which is a true and correct image of the browser and ActiveX dialog windows.*)

134. Although the browser window instructed me to "Click "YES" in the box," I clicked "No" to reject the download. A pop-up window appeared to indicate I "must click <YES> to access the site." *(See Exhibit F-7, which is a true and correct image of the windows.*)

135. I clicked "OK" to close the pop-up window and was again presented with the ActiveX dialog box asking if I wanted to install and run "http://www.thepaymentcentre.com/build/vciewer.cab" distributed by Holistyc Limited. *(See Exhibit F-8, which is a true and correct image of the browser and ActiveX dialog windows.*)

136. Again, I clicked "No" to reject the download and was unable to advance. When presented with the ActiveX dialog box for the third time, I clicked "Yes" to proceed. The dialog box closed. *(See Exhibit F-9, which is a true and correct image of the browser window.*)

137. Moments later, a new browser window launched, one with the address bar hidden, entitled "Gruesome - Internet." *(See Exhibit F-10, which is a true and correct image of the browser window.)*

138. Despite offering a dropdown menu to "Choose your country," there were no choices from which to select. *(See Exhibit F-11, which is a true and correct image of the browser window and dropdown menu.)*

139. I attemped to close the window by clicking on the X in the upper right corner and a pop-up window appeared to confirm I wanted to quit. *(See Exhibit F-12, which is a true and correct image of the browser and pop-up window.)*

140. I clicked "Yes" to exit and the "Gruesome - Internet" window closed, immediately

followed by two new window launches: <www.hotmovies.com> and <www.xxxporn.com.22545.fb.dbbsrv.com>. *(See Exhibit F-13, which is a true and correct image of the windows.)*

141. I closed both browser windows, revealing the Windows Desktop beneath. Since the <www.thepaymentcentre.com> download, two new icons were added to the display: "Gruesome" and "Ring Tones & Logos." *(See Exhibit F-14, which is a true and correct image of the Desktop.)*

142. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. The scan identified 68 new critical objects, including 34 attributed to VX2 and 20 to Holystic-Dialer. In addition, Ad-Aware identified 6 Possible Browser Hijack attempts associated with <www.abetterinternet.com>. Spybot identified 15 problems, including entries for both "AbetterInternet." and "Holistyc." (*See Exhibit F-15, which are true and correct images of the relevant scan results.*)

143. Despite the obvious addition of new programs, I opened the C:\Program Files\ folder, which indicated the same seventeen files as prior to the Holistyc download. Neither Holystic nor Direct Revenue's Aurora program were listed. *(See Exhibit F-16, which is a true and correct image of the window.*)

144. I proceeded to the C:\WINDOWS folder, which indicated that several files had been newly added to that directory, including the Direct Revenue files "Nail" and "svcproc." The listed "Date Modified" for the files was January 21, 2005 and May 12, 2002, respectively. *(See Exhibit F-17, which are true and correct images of the window.*)

145. I next opened the C:\WINDOWS\System32 folder, which also indicated the

addition of several new files, including the Direct Revenue file "DrPMon.dll" and the seemingly randomly named "exjxtv." The listed "Date Modified" for each file was July 6, 2003 and January 18, 2002, respectively. *(See Exhibit F-18, which are true and correct excerpted images of the windows.)*

146. I launched Internet Explorer, which was set to open <www.msn.com>. Upon loading that page, a pop-up window promptly displayed an Aurora-branded pop-up advertisement for "free Registry Cleaner software" by SysTweak.com. *(See Exhibit F-19, which is a true and correct image of the browser and pop-up windows.*)

147. Within five minutes of running searches on Google for job-related terms and visiting sites such as <hotjobs.yahoo.com> and <www.monster.com>, I received three Aurora-branded popups: one for Napster, and two for career-related websites. *(See Exhibit F-20, which are true and correct images of the browser and pop-up windows.*)

AIMPhuck.com "Emoticon Download Manager" download

148. On January 27, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit G-1, which are true and correct images of the result screens.)*

149. I opened the Program Files folder to record the seventeen files located with that folder. (*See Exhibit G-2, which is a true and correct image of the window.)*

150. I opened Internet Explorer and directed the browser to <www.aimphuck.com>. Immediately, an ActiveX dialog offering the installation of "A FREE Emoticon Download

Manager" distributed by "NicTech Networks Inc." appeared on the screen over the browser window. *(See Exhibit G-3, which is a true and correct image of the browser and ActiveX windows.)*

151. I clicked "No" to decline the installation and a received a pop-up window notice that "In order to access the site You must click YES." *(See Exhibit G-4, which is a true and correct image of the browser and pop-up windows.)*

152. I clicked "OK" to close the pop-up window and another ActiveX dialog box launched asking if I wanted to "install and run 'Macromedia Flash Player 7.'" *(See Exhibit G-5, which is a true and correct image of the browser and ActiveX windows.)*

153. I selected "No" to decline the Macromedia installation and the first viewed ActiveX Security Window re-launched, offering "A FREE Emoticon Download Manager" distributed by "NicTech Networks Inc." *(See Exhibit G-6, which is a true and correct image of the browser and ActiveX windows.)*

154. I again clicked "No" to reject the download, closing the ActiveX dialog box. Despite this, a message appeared in the lower left corner of the Internet Explorer browser window to indicate: "Installing components...Imbum_bw.cab." I was not presented with any license agreement prior to this installation, nor had there been any obvious link any terms and conditions of the download. *(See Exhibit G-7, which is a true and correct image of the browser window.)*

155. Another box launched with the message, "This is a 1 time install, once you click Open it will never pop up this message again." In the main Internet Explorer window, the message at the bottom of the screen continued to indicate the installation of "Imbum_bw.dll."

(See Exhibit G-8, which is a true and correct image of the browser and pop-up windows.)

156. I clicked "OK" to close the box and was served two pop-up windows to commence download of the file "Imbum_exe from www.aimphuck.com." *(See Exhibit G-9, which is a true and correct image of the browser and pop-up windows.)*

157. I then selected a location for the application to be saved. *(See Exhibit G-10, which is a true and correct image of the windows.)*

158. A window popped up to indicate the progress of the download, and I received notification when the download was complete. *(See Exhibit G-11, which is a true and correct image of the windows.)*

159. I clicked "Open" to initiate the program, and without further action on my part, all the windows automatically closed. A warning window launched over the Windows desktop, titled "msg116" and containing no text other than a yellow triangle with a black exclamation mark. *(See Exhibit G-12, which is a true and correct image of the Desktop.)*

160. At that point, I attempted to run the Ad-Aware and Spybot checks for spyware, but shortly into the scans, the machine became unresponsive and the computer generated the Windows general protection fault error message over a blue screen. I was forced to power off the computer and restart manually.

161. After rebooting several times, I opened the C:\Program Files\ folder for a listing of its contents. Six new folders had been added since downloading the NicTech Networks emoticon download manager: "AdDestroyer," "eZula," "Recommended Hotfix - 421701D," "SED," "Vbouncer" and "Web Offer." No Direct Revenue spyware program was listed. *(See Exhibit G-13, which is a true and correct image of the window.)*

162. I then entered the Windows "Add or Remove Programs" utility to view the list of currently installed programs. The listing included unfamiliar programs that I did not actively agree to accept, including "AdDestroyer,""DMVlite," "Recommended Hotfix - 421701D," "TopText iLookup," "Virtual Bouncer" and "Web Offer." Again, no Direct Revenue spyware program was listed. *(See Exhibit G-14, which is a true and correct image of the window.)*

163. I closed the utility, and opened the Internet Explorer window. Without visiting any new web pages, I was served with five pop-up advertisements. Because none of the ads were branded, I could not identify what program(s) had generated them. *(See Exhibit G-15, which are true and correct images of the browser windows.)*

164. I reloaded both Ad-Aware and Spybot programs onto the computer to run scans for existing spyware. The Ad-Aware scan identified 464 objects, 14 attributable to VX2, including registry keys, registry values, files and two running processes. (*See Exhibit G-16, which are true and correct images of the relevant scan results.*)

165. I then ran a scan on the unit's hard drive with Spybot. That search identified 172 problems, including one entry for "VX2/h.AbetterInternet." (*See Exhibit G-17, which is a true and correct image of the relevant scan results.*)

Wallpapers4U.com download

166. On September 1, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit H-1, which are true and correct images of the result screens.)*

167. I then opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit H-2, which is a true and correct image of the window.)*

168. I proceeded to the C:\WINDOWS folder to view a listing of the files located within that folder. *(See Exhibit H-3, which are true and correct images of the windows.)*

169. Within the C:\WINDOWS folder, I opened the System32 folder to view a listing of its contents. *(See Exhibit H-4, which are true and correct excerpted images of the window.)*

170. Finally, I captured an image of the Windows Desktop, prior to any downloads. *(See Exhibit H-5, which is a true and correct image of the Desktop.)*

171. I launched Internet Explorer and directed the browser to <www.wallpapers4u.com>. The page began loading and a Privacy window popped up to indicate that the site's cookie had been restricted based on my computer's privacy settings. *(See Exhibit H-6, which is a true and correct images of the windows.)*

172. I clicked "OK" to close the Privacy window and the browser window froze and became unresponsive. I closed the browser window through the Windows Task Manager (accessed by clicking Ctrl-Alt-Delete) and re-launched Internet Explorer. Upon directing the browser to <www.wallpapers4u.com>, I was served with an Aurora-branded pop-up advertisement listing several auto insurance companies. *(See Exhibit H-7, which is a true and correct image of the windows.)*

173. When I attempted to close the Aurora advertisement, the browser windows froze and again became unresponsive. I again closed the browser windows through the Windows Task Manager, revealing the Desktop. After merely visiting the <www.wallpapers4u.com> website, five new icons were added to the Desktop: Download Free Movies, Free Platinum Card, Kill All

Spyware, Play Bingo Free Money and Virus Hunter. In addition, a "Windows Security Alert" window launched, indicating that "Virtual Bouncer has found Aurora on your computer" and offering the option to remove the "parasite" from my computer. *(See Exhibit H-8, which is a true and correct image of the Desktop.)*

174. I entered the Windows "Add or Remove Programs" utility to view the list of currently installed programs. The listing included "The ABI Network - A Division of Direct Revenue" as well as "InternetOffers," "PShow," "Surf SideKick," "The Best Offers," "Tokuoitu," and "Virtual Bouncer." (*See Exhibit H-9, which is a true and correct image of the window.*)

175. I opened the C:\Program Files\ folder, which indicated that thirteen new files had been added after visiting the <www.wallpapers4u.com> website: "180searchassistant," "BullsEye Network," "Internet Optimizer," "ISTsvc," "Media Gateway," "Personal Money Tree," "Power Scan," "Quick Links," "SideFind," "SurfAccuracy," "SurfSideKisk 3," "Vbouncer" and "YourSiteBar." Direct Revenue's Aurora program was not listed. *(See Exhibit H-10, which are true and correct images of the window.*)

176. I proceeded to the C:\WINDOWS folder, which indicated that many files had been newly added to that directory, including the Direct Revenue files "Nail" and "svcproc." The listed "Date Modified" for each of the files was May 11, 2005 and June 11, 2003, respectively. *(See Exhibit H-11, which are true and correct images of the window.*)

177. The C:\WINDOWS\System32 folder also indicated the addition of many new files. *(See Exhibit H-12, which are true and correct excerpted images of the window.*) However, the computer's system became unstable at that point, and the unit ceased to respond to further

input, ending further tests.

STLyrics.com "FlashTalk" download attempt

178. On February 2, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit I-1, which are true and correct images of the result screens.)*

179. I opened the C the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit I-2, which is a true and correct image of the window.)*

180. I launched Internet Explorer and directed the browser to the Google search engine at <www.google.com>. I typed "bye bye birdie lyrics" into the search bar and hit "Search." Among the results, the second listed the page titled "Bye Bye Birdie Soundtrack Lyrics [2000] Musical Bye Bye Birdie...", located at <www.stlyrics.com/b/byebyebirdie.htm>. *(See Exhibit I-3, which is a true and correct excerpted image of the search results window.)*

181. I clicked on that link and was directed to a page over which an ActiveX dialog box appeared asking if I wanted to install and run "IE PLUGIN - Browser Plugin" distributed by "IE PLUGIN LTD." *(See Exhibit I-4, which is a true and correct image of the browser and ActiveX dialog windows.*)

182. I clicked "No" to reject the installation and another ActiveX dialog box launched asking if I wanted to install and run a "game from the BullsEye Game Network" distributed by "eXact Advertising." *(See Exhibit I-5, which is a true and correct image of the browser and ActiveX dialog windows.*)

183. I clicked "No" again and was served with a third ActiveX dialog box asking if I wanted to install and run "the latest version of FlashTalk" distributed by "BetterInternet." The dialog indicated that clicking "Yes" would acknowledge acceptance and understanding of BetterInternet's Consumer Policy Agreement. *(See Exhibit I-6, which is a true and correct image of the browser and ActiveX dialog windows.*)

184. At no point in this process was an active viewing of the BetterInternet Consumer Policy agreement required to advance. I clicked "Yes" to proceed with the installation, closing the ActiveX dialog. *(See Exhibit I-7, which is a true and correct excerpted image of the browser window.*)

185. After no visible change to the display for several minutes, I closed all browser windows and opened the C:\Program Files\ folder, which indicated that no new files had been added to the pre-existing seventeen files. *(See Exhibit I-8, which is a true and correct image of the window.*)

186. I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 12 new critical objects, 5 attributed to VX2 files, a registry value and a process. (*See Exhibit I-9, which are true and correct images of the scan results.*)

187. The scan by Spybot identified 9 problems, including 1 entry for Callinghome.biz. (*See Exhibit I-10, which is a true and correct image of the scan results.*)

JenniferLopez.net download

188. On November 18, 2004, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive, using the Ad-Aware and Spybot programs. At that time, the programs

indicated the hard drive to be free of spyware. *(See Exhibit J-1, which are true and correct images of the result screens.)*

189. I next opened the C:\Program Files folder to view a listing of the eighteen files located within that folder. *(See Exhibit J-2, which is a true and correct image of the window.)*

190. I opened Internet Explorer and directed the browser to <www.google.com>. In the Google.com search bar, I entered in a search for "jenniferlopez." The <JenniferLopez.net> site was among the first sites returned. *(See Exhibit J-3, which is a true and correct image of the browser window.)*

191. I clicked on the hyperlink for "Jennifer Lopez JLo > pictures, wallpaper, pics, movies, videos ..." and was directed to the <JenniferLopez.net> homepage. Neither this page – nor any other on the JenniferLopez.net site – made any mention of bundled spyware programs. As the page was being opened, an ActiveX Security Warning window popped up asking if I wanted to "install and run 'Macromedia Flash Player 7.'" *(See Exhibit J-4, which is a true and correct image of the browser window and pop-up window.)*

192. I clicked "No" and the <JenniferLopez.net> homepage continued to load. *(See Exhibit J-5, which is a true and correct image of the browser window.)*

193. I clicked on the hyperlink for "Gallery" and was directed to the "Jennifer Lopez JLo Gallery" page. As the page was loading, I again received the ActiveX dialog asking if I wanted to "install and run 'Macromedia Flash Player 7.'" In the meantime, in the lower left corner of the Internet Explorer browser window, the message appeared, reading: "Installing components...baeor05.cab." *(See Exhibit J-6, which is a true and correct image of the browser window and pop-up window.)*

194. I clicked "No" in the window and another ActiveX Security Warning window popped up, asking if I wanted to "install and run 'FREE on-line games and special offers from Addictive Technologies Partners. In addition, get cash back on your online purchases from Shop at Home Select.'" *(See Exhibit J-7, which is a true and correct image of the browser window and pop-up window.)*

195. I clicked "No" in the window and a box appeared with the message, "To install latest AT-Games update, please click YES." *(See Exhibit J-8, which is a true and correct image of the browser window and pop-up window.)*

196. I clicked "OK" to close the box and was served again with the ActiveX dialog asking if I wanted to install and run "FREE on-line games and special offers from Addictive Technologies Partners." In the lower left corner of the Internet Explorer browser window, the message again appeared: "Installing components...baeor05.cab." *(See Exhibit J-9, which is a true and correct image of the browser window and pop-up window.)*

197. As I had before, I clicked "No" in the window and a box appeared with the message, "This is a 1 time install, once you click Open it will never pop up this message again." *(See Exhibit J-10, which is a true and correct image of the browser window and pop-up window.)*

198. I clicked "OK" to close the box and was served two pop-up windows to commence download of the file "baeor05.exe from www.addictivetechnologies.net." *(See Exhibit J-11, which is a true and correct image of the browser window and pop-up windows.)*

199. I clicked "Cancel" within the pop-up window and closed all browser windows without agreeing to any download. I then opened the C:\Program Files folder for a listing of the

files located within that folder. This listing indicated that four new folders had been added after my visit to the JenniferLopez.net website: IncrediFind, MEGASEAR TOOLBAR, TV Media and Web_Rebates. Direct Revenue's program was not among those listed. *(See Exhibit J-12, which is a true and correct image of the window.)*

200. I closed the Program Files folder and ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan turned up 230 objects, including several VX2 registry keys and values, files and a folder. *(See Exhibit J-13, which are true and correct excerpted images of the scan results.)*

201. I then ran a scan for existing spyware on the unit's hard drive with Spybot. That scan identified 62 problems, including 5 entries for VX2/e. *(See Exhibit J-14, which is a true and correct images of the relevant scan results.)*

202. I ran this same test three other times over two days, removing all identified spyware in between each test, and achieved similar results each time. After every test, both Ad-Aware and Spybot scans indicated the surreptitious addition of VX2 files to my hard drive. In fact, VX2 was one of the few consistent additions to the hard drive, appearing after all four scans even when other programs did not. *(See Exhibits J-15, J-16 and J-17, which are true and correct images of the relevant scan results for each test.)*

PCWeatherAlert download

203. On February 7, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive, using the Ad-Aware and Spybot programs. At that time, the programs indicated the hard drive to be free of spyware. *(See Exhibit K-1, which are true and correct*

images of the result screens.)

204. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. *(See Exhibit K-2, which is a true and correct image of the window.)*

205. I opened Internet Explorer and in the address bar typed in <www.weatherblaster.com>. The browser directed automatically to the PC WeatherAlert.com website at <www.pcweatheralert.com>. Neither this page – nor any other leading up to the download of the PCWeatherAlert software – made any mention of bundled spyware programs. *(See Exhibit K-3, which are true and correct images of the browser window.)*

206. In the "Download Area" of the homepage, I clicked on the button to "Download Now!" and received a pop-up indicating the status of the download. *(See Exhibit K-4, which is a true and correct image of the browser window and pop-up window.)*

207. I then received a pop-up Security Warning window asking, "Do you want to install and run 'Quick Installer provides a comprehensive, safe, secure, end-to-end software delivery installation suite.' *[sic]*" *(See Exhibit K-5, which is a true and correct image of the browser window and pop-up window.)*

208. I clicked "Yes" in the Security Warning window, and the window closed. *(See Exhibit K-6, which is a true and correct image of the browser window and pop-up window.)*

209. The PCWeatherAlert Downloader progress window confirmed completion of the download and a new "PC WeatherAlert 1.0 Setup" window launched beneath. *(See Exhibit K-7, which is a true and correct image of the browser window and pop-up window.)*

210. Without further action, I received a pop-up window indicating completion of "WebRebates_Install Setup." *(See Exhibit K-8, which is a true and correct image of the browser*

window and pop-up window.)

211. I clicked the "Close" button to exit the WebRebates installation window and was able to view the first screen of the "PCWeatherAlert 1.0 Setup" window. *(See Exhibit K-9, which is a true and correct image of the browser window and pop-up window.)*

212. I then clicked "Next" to continue the installation and was directed to a screen requesting a location for the PCWeatherAlert installation. *(See Exhibit K-10, which is a true and correct image of the browser window and pop-up window.)*

213. Leaving the location at the default setting, I clicked "Next" to continue and was directed to a screen to choose a Start Menu folder for the PCWeatherAlert program's shortcuts. *(See Exhibit K-11, which is a true and correct image of the browser window and pop-up window.)*

214. Also leaving the folder name at the default setting, I clicked "Next" and was directed to the final installation screen. *(See Exhibit K-12, which is a true and correct image of the browser window and pop-up window.)*

215. I clicked the "Install" button to complete installation and received onscreen confirmation that "PCWeatherAlert has been installed on your computer." *(See Exhibit K-13, which is a true and correct image of the browser window and pop-up window.)*

216. I clicked on the "Finish" button and received a pop-up window for the PC Weather Alert sign up. *(See Exhibit K-14, which is a true and correct image of the browser window and pop-up window.)*

217. I attempted to advance without providing any personal information by clicking "OK," but was unable to proceed without providing name and email address. I submitted the

information as required, and clicked "OK" to continue. The PC Weather Alert program launched in a new window. *(See Exhibit K-15, which is a true and correct image of the window.)*

218. I next opened C:\Program Files for a listing of the files located within that folder. The listing indicated that seven files had been added during the "PC Weather Alert" download process: BullsEye Network, PCWeatherAlert, NaviSearch, CashBack, Bargain Buddy, IncrediFind and Web_Rebates. Direct Revenue's spyware was not listed among the newly added programs. *(See Exhibit K-16, which is a true and correct image of the window.*)

219. I closed Internet Explorer and launched the Windows "Add or Remove Programs" utility through the Windows Control Panel and was offered the option to remove CashBack by BargainBuddy, NaviSearch, The BullsEye Network, WebRebates (by TopRebates.com) and WebSpecials, but no Direct Revenue program. *(See Exhibit K-17, which is a true and correct image of the window.)*

220. I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan turned up 371 objects, including a VX2 process, registry value and file. *(See Exhibit K-18, which are true and correct excerpted images of the scan results.)*

221. I followed this with a scan for existing spyware using Spybot. That scan identified 78 problems, including 1 entry for Direct Revenue's CallingHome.biz. *(See Exhibit K-19, which is a true and correct image of the relevant scan results.)*

TaskBuddy.com download

222. On February 25, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive, using the Ad-Aware and Spybot programs. At that time, the programs

indicated the hard drive to be free of spyware. *(See Exhibit L-1, which are true and correct images of the result screens.)*

223. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. *(See Exhibit L-2, which is a true and correct image of the window.)*

224. I launched Internet Explorer and in the address bar typed in <www.taskbuddy.com>. The browser directed automatically to TaskBuddy's homepage. Neither this page – nor any other leading up to the download of the TaskBuddy software – made any mention of bundled spyware programs. *(See Exhibit L-3, which are true and correct images of the browser window.)*

225. At the bottom of the homepage, I clicked on the link to the "Terms of Use." A new window launched with the "terms of use and end user license agreement for Taskbuddy.com software and web site." The actual text of the agreement, however, was obscured by appearing as white print on a white background. *(See Exhibit L-4, which are true and correct images of the browser window.)*

226. Only by highlighting the text with the cursor was I able to view and scroll through the entire agreement over 12 screens. *(See Exhibit L-5, which are true and correct images of the highlighted text within the browser window.)*

227. I returned to the Taskbuddy.com homepage and clicked on the button for download. A pop-up window launched, displaying the first eleven lines of the TaskBuddy End User License Agreement. By scrolling through the window – which could not be enlarged – I was able to view the entire agreement over seventeen screens. The license agreement did not mention Direct Revenue or any bundled spyware programs. *(See Exhibit L-6, which are true and*

correct images of the browser window and pop-up window.)

228. I agreed to the terms by checking the box at the bottom of the window and clicked "Continue." A Security Warning window popped up asking, "Do you want to install and run 'Quick Installer provides a comprehensive, safe, secure, end-to-end software delivery installation suite.'*[sic]*" *(See Exhibit L-7, which is a true and correct image of the browser window and pop-up window.)*

229. I clicked "No" to decline the installation and the window closed, revealing the TaskBuddy Downloader window beneath. *(See Exhibit L-8, which is a true and correct image of the browser window and pop-up window.)*

230. Without further action, I was again presented with the Security Warning pop-up window asking to install "Quick Installer." *(See Exhibit L-9, which is a true and correct image of the browser window and pop-up window.)*

231. This time, I clicked "Yes" to accept the installation and the window closed, again revealing the TaskBuddy Downloader window. *(See Exhibit L-10, which is a true and correct image of the browser window and pop-up window.)*

232. Another pop-up window launched indicating completion of "WebRebates_Install Setup." *(See Exhibit L-11, which is a true and correct image of the browser window and pop-up window.)*

233. I clicked the "Close" button to exit the WebRebates installation window. An error window popped up indicating a RUNDLL error loading the "webspec.dll." *(See Exhibit L-12, which is a true and correct image of the browser window and pop-up window.)*

234. I clicked "OK" to close the error window and was served another pop-up window

to download the "Free GoldenRetriever software." *(See Exhibit L-13, which is a true and correct image of the browser window and pop-up window.)*

235. In the background, the TaskBuddy Installation wizard launched. *(See Exhibit L-14, which is a true and correct image of the browser window and pop-up window.)*

236. I clicked "Exit" to decline installation of the GoldenRetriever software and was presented with the first window of the TaskBuddy setup program. *(See Exhibit L-15, which is a true and correct image of the window.)*

237. I clicked "Next" to continue and was directed to a screen requesting a destination location for the program. *(See Exhibit L-16, which is a true and correct image of the window.)*

238. Leaving the location at the default setting, I clicked "Next" to continue and was directed to a screen requesting a location for the TaskBuddy icons. *(See Exhibit L-17, which is a true and correct image of the window.)*

239. Again leaving the setting at default, I clicked "Next" to advance to the next screen in the setup. *(See Exhibit L-18, which is a true and correct image of the window.)*

240. As directed, I clicked "Next"to begin installation and received onscreen confirmation that "TaskBuddy has been successfully installed." (*See Exhibit L-19, which is a true and correct image of the window.)*

241. I clicked on the "Finish" button and received a pop-up window for the TaskBuddy Registration. *(See Exhibit L-20, which is a true and correct image of the window.)*

242. I provided the required information, clicked "Register," and received a pop-up message confirming the registration. *(See Exhibit L-21, which is a true and correct image of the window, with identifying information redacted.)*

243. I clicked "OK" and the TaskBuddy program launched. *(See Exhibit L-22, which is a true and correct image of the desktop.)*

244. I closed all windows and opened C:\Program Files for a listing of the files located within that folder. The listing indicated that seven files had been added during the TaskBuddy download process: BullsEye Network, TaskBuddy, NaviSearch, CashBack, Bargain Buddy, IncrediFind and Web_Rebates. Direct Revenue's program was not among those listed. *(See Exhibit L-23, which is a true and correct image of the window.*)

245. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan turned up 370 objects, including a VX2 process, registry value and file. *(See Exhibit L-24, which is a true and correct image of the relevant scan results.)*

246. I followed this with a scan for existing spyware using Spybot. That scan identified 76 problems, including 2 entries for CallingHome.biz. *(See Exhibit L-25, which is a true and correct image of the relevant scan results.)*

247. I launched the Windows "Add or Remove Programs" utility through the Windows Control Panel and was offered the option to remove CashBack by BargainBuddy, NaviSearch, TaskBuddy, The BullsEye Network, WebRebates (by TopRebates.com) and WebSpecials. No Direct Revenue programs were listed. *(See Exhibit L-26, which is a true and correct image of the window.)*

Crackz.ws download

248. On May 19, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran scans for existing spyware on the computer's hard drive using Ad-Aware and Spybot. At that time, the programs indicated the hard drive to be free

of spyware. (*See Exhibit M-1, which are true and correct images of the result screens.)*

249. I opened the C:\Program Files\ folder to view a listing of the seventeen files located within that folder. *(See Exhibit M-2, which is a true and correct image of the window.)*

250. I proceeded to the C:\WINDOWS folder to view a listing of the files located within that folder. *(See Exhibit M-3, which are true and correct images of the windows.)*

251. Within the C:\WINDOWS folder, I opened the System32 folder to view a listing of its contents. *(See Exhibit M-4, which are true and correct excerpted images of the window.)*

252. I next opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit M-5, which is a true and correct image of the browser window*.)

253. Finally, I captured an image of the Windows Desktop, prior to visiting the target site. *(See Exhibit M-6, which is a true and correct image of the Desktop.)*

254. I directed the browser to <www.crackz.ws> immediately received an "Install on Demand" box for downloading "Java virtual machine." Beneath the main window, another window launched for the website "fuck-access.com." *(See Exhibit M-7, which is a true and correct image of the window.)*

255. Before I could take additional action, both browser windows closed automatically, revealing the Windows Desktop to which several new items (for "Virus Hunter Security" and "Spyware Avenger," and more cryptic titles as "1," "3," "4," "5,") began being added. A warning window of indeterminate origin popped up over the desktop as well, advising that "You must click YES to continue." Still without my taking any action, additional files and icons continued to be added to the desktop, and the desktop background revealed that a fatal error had occurred. I received a pop-up box indicating that "Dialing failed." *(See Exhibit M-8, which are*

true and correct images of the Desktop.)

256. At that point, I received several pop-ups on the desktop: one for "Cash Back software from ShopAtHomeSelect.com," one for "spam protection" software intended to mimic the appearance of an email Inbox with a warning window indicating "too much SPAM!" and an ActiveX dialog for"free gaming software" from Crazywinnings Inc. I closed all the windows without agreeing to any installations. *(See Exhibit M-9, which are true and correct images of the Desktop.)*

257. I entered the Windows "Add or Remove Programs" utility to view the list of currently installed programs. The listing included "Internet Optimizer, "Search Assistant Uninstall," "Security iGuard," "Select Cashback," "TContext," "The BullsEye Network," "UCmore - The Search Accelerator," "WebSearch Toolbar" and "Win-Tools Easy Installer (by WebSearch)." Direct Revenue's Aurora program was not listed. (*See Exhibit M-10, which is a true and correct image of the window.*)

258. I opened the C:\Program Files\ folder, which indicated that seven new files had been added since my visit to <www.crackz.ws>: "AutoUpdate," "BullsEye Network," "Internet Optimizer," "Security iGuard," "TheSearchAccelerator," "Toolbar" and "WebSiteViewer." Direct Revenue's Aurora program was not among those listed. *(See Exhibit M-11, which is a true and correct image of the window.*)

259. I proceeded to the C:\WINDOWS folder, which indicated that many files had been added to that directory, including the Direct Revenue files "twain_32.dll" and "Nail." Although these files had just been installed, the "Date Modified" was listed as August 23, 2001 and October 10, 2000, respectively. *(See Exhibit M-12, which are true and correct images of the*

windows.)

260. I next opened the C:\WINDOWS\System32 folder, which also indicated the addition of many files. *(See Exhibit M-13, which are true and correct excerpted images of the windows.)*

261. I closed the directory, revealing the Windows Desktop beneath. Since the <www.crackz.ws> visit, a total of eighteen new object had been added to the display: "1," "2," "3," 4," "5," "6," "7," "4324ascsc32," "e342r323434r3," "e342e34e3," "uu.u," "testpage," "sex," "Virus Hunter Security," Spyware Avenger" and "Security iGuard." *(See Exhibit M-14, which is a true and correct image of the Desktop.)*

262. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware. The scan identified 705 new critical objects, including many VX2 registry keys and values, files, a folder and a running process. (*See Exhibit M-15, which are true and correct images of the relevant scan results and samples of the "Object Details" information provided by Ad-Aware.*)

263. Spybot identified128 problems, including 2 entries for "AbetterInternet" and 1 entry for "Callinghome.biz". (*See Exhibit M-16, which is a true and correct image of the relevant scan results.*)

264. I opened a new browser window through Internet Explorer and found the start page changed to <www.hsncnfkeol.biz>. (*See Exhibit M-17, which is a true and correct image of the browser window.*)

265. A pop-up window titled "Aurora" displayed an advertisement for online casino site <www.888.com>. Within ten minutes of surfing various travel-related websites, I received three additional Aurora-branded pop-up windows: one for United Airlines, one for priceline.com

and a third that contained no advertiser information. (*See Exhibit M-18, which are true and correct images of the browser and pop-up windows.*)

Search engine results: "aurora," "ceres," "offeroptimizer"

266. On July 6, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I launched Internet Explorer and directed the browser to the Google search engine at <www.google.com> to search for web pages related to "aurora," "ceres" and "offeroptimizer."

267. I typed "aurora" into the search bar and hit "Search." Among the first page of results, not one identified "myPCtuneup.com," the website Direct Revenue created to distribute the program for removing their spyware from users' computers.

268. I then ran Google searches for the terms "aurora spyware" and "remove aurora," neither of which identified "myPCtuneup.com" on the first page of results. Rather, many of the results appeared to be links to anti-spyware websites, or posted user complaints about the difficulty of removing Direct Revenue spyware from computers.

269. I repeated the searches for the terms "ceres," "ceres spyware," "remove ceres," "offeroptimizer," offeroptimizer spyware," and "remove offeroptimizer." As with the previous searches, none of the results identified the link to Direct Revenue's removal software at "myPCtuneup.com." *(See Exhibit N-1, which are true and correct images of the Google search results screen.*)

270. On July 29, 2005, I once again logged onto the internet from an undercover computer located at 120 Broadway, New York, New York. I ran the same searches for "aurora," "aurora spyware," "remove aurora," "ceres," "ceres spyware," "remove ceres," "offeroptimizer,"

"offeroptimizer spyware," and "remove offeroptimizer" through the popular Yahoo! and AskJeeves Internet search engines. As with the Google searches, none of the eighteen searches identified "myPCtuneup.com" among the first page of results. *(See Exhibits N-2 and N-3, which are true and correct images of the Yahoo and AskJeeves search results screens, respectively.*)

I declare under penalty of perjury that the forgoing is true and correct.

Executed on April __, 2006.

_____
Vanessa Ip
Investigator
New York State Office of the Attorney General
Internet Bureau
120 Broadway
New York, New York 10271

Sworn to before me
this ___ day of April 2006.

_____
Karen Geduldig
Notary Public